
White Collar Defense & Investigations and Securities Litigation & Enforcement
Client Service Groups and Data Privacy & Security Team

To: Our Clients and Friends

February 6, 2012

FINRA Issues Guidance on Protection of Customer Accounts

A recent alert from the Financial Industry Regulatory Authority ("FINRA") is encouraging broker-dealers to reexamine their policies and procedures relating to protection of customer assets and accounts.

FINRA Regulatory Notice 12-05 advises broker-dealers that FINRA has received an increasing number of reports of customer funds being stolen as a result of instructions e-mailed to firms from customer e-mail accounts that have been compromised. With that notice, FINRA, which regulates all broker-dealers, also issued a January 26, 2012 Investor Alert advising the public about these recent reported incidents, and recommending steps customers should take if they believe their e-mail account has been compromised.

In Notice 12-05, FINRA chronicles a recent trend in which customer e-mail accounts are compromised, the perpetrator assumes the e-mail identity of the real customer, and then sends an e-mail instruction to the broker-dealer to wire funds from the account to a third-party account. The firm, having received the instruction from the known e-mail address of the customer, follows the instructions and wires the funds. In some cases, perpetrators have sent phony letters of authorization, which are also e-mailed from the compromised customer account.

In at least one instance, in an apparent attempt to avoid questioning from the firm, the e-mail stressed that the customer had a family emergency, would consequently be unavailable to discuss the request, and needed to have the funds transferred immediately.

FINRA reminds firms in Notice 12-05 that under FINRA Rule 3012 (which became effective on January 31, 2005), they should have supervisory controls to protect customer funds. This Rule requires all firms to establish written supervisory control policies and procedures that, among other things, include procedures that are reasonably designed to review and monitor the transmittal of funds, including those transmitted by wire or check, in the following types of instances:

- from customer accounts to third-party accounts (i.e., a transmittal that would result in a change of beneficial ownership);
- from customer accounts to outside entities (e.g., banks, investment companies);

- from customer accounts to locations other than a customer’s primary residence (e.g., post office box, “in care of” accounts, alternate address); and
- between customers and registered representatives (including the hand-delivery of checks).

Rule 3012 expressly states, and Regulatory Notice 12-05 serves as a reminder, that these policies and procedures “must include a means or method of customer confirmation, notification, or follow-up that can be documented.” It follows that because customer e-mail accounts are susceptible to being hacked, a firm that accepts customer instructions via e-mail may be required to deal with that risk in its supervisory systems and procedures.

Regulatory Notice 12-05 and the accompanying FINRA Investor Alert are just the latest reminders FINRA has given on this subject. Regulatory Notice 09-64, released in November 2009, notified firms that they must enforce policies and procedures governing the transmittal of funds or other assets from customer accounts. The notice said firms should test and verify their procedures and update them when necessary.

FINRA began issuing guidance to firms as early as July 2005 on the broader concept of protection of customer information and assets, and has been issuing Investor Alerts since that time. Further, the Federal Bureau of Investigation, Financial Services Information Sharing and Analysis Center, and Internet Crime Complaint Center recently released a joint fraud alert describing a similar trend in thefts using e-mail accounts.

In the past, FINRA and the Securities and Exchange Commission have issued these types of alerts as a precursor to a heightened focus on an activity through the examinations and, potentially, enforcement actions.

Given the gravity of potential customer harm and reputational risk for firms, coupled with the repeated emphasis by regulators and law enforcement on this issue, regulators are likely to give close scrutiny to firms’ systems and procedures for safeguarding customer assets. In particular, firms that accept, via e-mail, customer instructions to promptly withdraw or transfer funds may well be asked to describe the preventive steps they employ in complying with these instructions. To prepare for such scrutiny, firms should consider providing robust training to all of their employees on the need to protect customer information, with special training for those employees involved in the process of accepting customer instructions and wiring funds.

For further information, please speak to your Bryan Cave contact, any member of the [Bryan Cave Data Privacy and Security Team](#), or the authors of this alert:

Jeffrey J. Kalinowski

314 259 2949

jeff.kalinowski@bryancave.com

Eric Rieder

212 541 2057

erieder@bryancave.com

Jeffrey A. Ziesman

816 374 3225

jeff.ziesman@bryancave.com

David A. Zetoony

202 508 6030

david.zetoony@bryancave.com

In addition, if you experience a data security breach and are not able to contact a member of the Team directly, you can call **Bryan Cave’s Data Breach Hotline** 24 hours a day, 7 days a week at 1-888-474-9743.